Mạng không an toàn
Phần 3: Thảm họa được tiên đoán — và bị bỏ qua

Các cảnh báo của L0pht về Internet đã lôi cuốn sự chú ý nhưng ít hành động

Tác giả Craig Timberg viết cho tờ Washington Post, xuất bản: 22/06/2015

Dịch sang tiếng Việt: Lê Trung Nghĩa, letrungnghia.foss@gmail.com

Dịch xong: 05/07/2015

Bản gốc tiếng Anh:

http://www.washingtonpost.com/sf/business/2015/06/22/net-of-insecurity-part-3/

Net of insecurity
Part 3: A disaster foretold — and ignored

L0pht’s warnings about the Internet drew notice but little action

Story by Craig Timberg for The Washington Post, published 06/22/2015

7 người trẻ tuổi ngồi trước vài nhà làm luật quyền lực nhất Đồi Capitol từng chưa phải là các sinh viên tốt nghiệp đại học hay các nhà phân tích trẻ tuổi từ vài nhóm nghiên cứu chiến lược. Không, Space Rogue, Kingpin, Mudge và những người khác từng là các tin tặc đã tới từ các vùng bí ẩn của không gian mạng để đưa ra một cảnh báo làm kinh sợ thế giới.

Máy tính của các ngài, họ đã nói cho nhóm các thượng nghị sỹ vào tháng 05/1998, là không an toàn - không phải phần mềm, không phải phần cứng, không phải các mạng mà liên kết chúng lại với nhau. Các công ty mà xây dựng các thứ đó không quan tâm, các tin tặc đã tiếp tục, và họ không có lý do gì để quan tâm vì sự thất bại không khiến họ mất gì cả. Và chính phủ liên bang không có kỹ năng cũng không có thiện chí làm bất kỳ điều gì với nó.

“Nếu các ngài đang tìm kiếm an toàn máy tính, thì Internet không phải là nơi để tìm”, Mudge, 27 tuổi, và trông giống như một nhà tiên tri trong kinh thánh với tóc nâu dài trải dài qua vai anh ta. Bản thân Internet, anh ta nói tiếp, có thể bị đánh sập “bởi bất kỳ cá nhân nào trong số 7 người ngồi trước mặt các ngài” với 30 phút gõ phím được dàn dựng tốt.

Các thượng nghị sỹ - một nhóm cả 2 đảng bao gồm John Glenn, Joseph I. Lieberman và Fred D. Thompson - trang nghiêm gật đầu, làm rõ rằng họ hiểu sự hấp dẫn của tình huống. “Chúng tôi sẽ phải làm gì đó về nó”, Thompson đã nói.

Thay vào đó những gì đã xảy ra từng là bi kịch của 1 cơ hội bị bỏ lỡ, và 17 năm sau thế giới vẫn còn trả giá cho sự mất an toàn quá đáng.

Sự làm chứng của L0pht, như nhóm tin tặc tự gọi mình, từng là sự bạo gan nhất của một dàn hợp xướng gia tăng các cảnh báo được phát ra vào những năm 1990 khi Internet từng bùng nổ về số lượng người, vâng theo cách của nó đang trở thành một lực lượng hùng mạnh toàn cầu cho truyền thông, thương mại và tội phạm.

Các tin tặc và các chuyên gia máy tính khác đã thấy các cảnh báo khi World Wide Web đã mang sức mạnh có tính biến đổi của việc kết nối mạng tới đại chúng. Điều này đã tạo ra một vũ trụ các rủi ro cho những người sử dụng và các hệ thống sống còn của thế giới thực, như các nhà máy điện, nhanh chóng cũng đi lên trực tuyến.

Các quan chức ở Washington và khắp thế giới đã thất bại để mạnh mẽ giải quyết các vấn đề như sự lan truyền đáng lo ngại khắp không gian

Câu chuyện của **Craig Timberg**

Video của **Jorge Ribas**

Xuất bản 22/06/2015

Tạo ra Internet bị tổn thương: Câu chuyện này là phần 3 của dự án nhiều phần về các chỗ bị tổn thương vốn dĩ của Internet và vì sao chúng có thể không bao giờ được sửa.

Phần 1: Câu chuyện Internet đã trở nên dễ bị tổn thương đến thế bằng cách nào

Phần 2: Sống lâu với 'sự sửa nhanh'

Ảnh: Xem tài liệu gốc

Các tin tặc của L0pht gồm: Brian Oblivion, Tan, Kingpin, Mudge, Weld Pond, Space Rogue và Stefan von Neumann làm chứng trước nhóm các Thượng nghị sỹ vào năm 1998. (Douglas Graham / Congressional Quarterly qua Getty Images)

mạng, một mặt trận mới khổng lồ cơ hội và tình trạng lộn xộn vô luật lệ. Thậm chí ngày nay, nhiều sự thâm nhập trái phép nghiêm trọng trên trực tuyến khai thác các lỗi trong các phần mềm trước hết được xây dựng trong kỷ nguyên đó, như Adobe Flash, Java của Oracle và Internet Explorer của Microsoft.

"Chúng ta có cùng y hệt các vấn đề về an toàn", Space Rogue, tên thật là Cris Thomas, đã nói. "Có nhiều tiền hơn được bỏ vào. Có sự nhận thức nhiều hơn. Nhưng các vấn đề y hệt vẫn còn đó".

L0pht, đã sinh ra trong cảnh tượng các tin tặc hối hả ở vùng Boston, nổi lên như một trận lụt các phần mềm mới đã giới thiệu những điều kỳ diệu như vậy như các trò chơi âm thanh, hoạt hình và tương tác cho Web. Các phần mềm này, chúng đã đòi hỏi sự truy cập tới các chức năng cốt lõi của từng máy tính của người sử dụng, cũng đã trao cho các tin tặc các cơ hội mới để điều khiển các máy tính từ ở xa.

Việc đột nhập vào các máy tính có kết nối mạng đã trở nên quá dễ mà Internet, lãnh địa từ lâu của các nhà khoa học và những người có sở thích duy tâm riêng, dần phát triển nhiễm bẩn với hầu hết sự thực dụng các nghề nghiệp: trộm cắt, lừa đảo, gián điệp và chiến binh không gian mạng. Họ đã khai thác các lỗi máy tính vì lợi nhuận hoặc lợi ích khác trong khi liên tục tìm kiếm các chỗ bị tổn thương mới.

Các công ty công nghệ đôi khi tranh nhau để sửa các vấn đề - thường sau khi các tin tặc hoặc các nhà nghiên cứu hàn lâm đã phát hiện ra chúng một cách công khai - nhưng ít các công ty có thiện chí triển khai sự đại tu cần thiết tốn kém để làm cho các hệ thống của họ an toàn hơn đáng kể chống lại các cuộc tấn công trong tương lai. Lợi nhuận của họ phụ thuộc vào các yếu tố khác, như việc cung cấp cho những người tiêu dùng các tính năng mới, chứ không phải canh giữ các tin tặc.

"Trong thế giới thực, mọi người chỉ đầu tư tiền để giải quyết các vấn đề thực, như đối nghịch với các vấn đề giả thuyết", Dan S Wallach, một giáo sư khoa học máy tính của Đại học Rice, người đã và đang nghiên cứu các mối đe dọa trực tuyến từ những năm 1990, nói. "Những thứ bạn đang bán là không an toàn. Những thứ bạn đang bán là những thứ gì khác đó nữa".

Kết quả là một văn hóa trong giới công nghiệp công nghệ thường bắt nguồn như "vá và cầu nguyện". Nói cách khác, giữ tiếp tục xây dựng, giữ tiếp tục bán và gửi đi các bản vá khi cần. Nếu một hệ thống hỏng -

gây ra mất dữ liệu, các số thẻ tín dụng bị ăn cắp hoặc các máy tính mất thời gian vì sập - thì gánh nặng không đặt lên những người khổng lồ, các công ty công nghệ giàu có, mà lên các khách hàng của họ.

Các thành viên của L0pth nói họ thường trải nghiệm thái độ ngạo mạn này trong các công việc hàng ngày của họ, nơi mà vài người đã mệt nhọc như các lập trình viên khiêm tốn hoặc những người bán hàng ở các cửa hàng máy tính. Khi họ báo cáo lỗi cho các nhà sản xuất phần mềm, các quan chức công ty thường hỏi: Liệu có ai đó khác biết về điều này không?

Ảnh: Xem tài liệu gốc

Peiter Zatko, tên hiệu là Mudge, từng thích thú trong việc vặn vẹo Microsoft khi anh ta đã mô tả việc phá an toàn mật khẩu của hãng trong Windows. Nhiều năm sau, sự suy tàn của L0pht đã đánh vào anh ta. (Nick Otto của The Washington Post).

Thiên đường của các lập trình viên trên cái gác xép ở Boston

Các tin tặc gặp nhau trên trực tuyến, hầu hết trong các bảng thông báo đã đưa ra cho những người nhiệt thành máy tính với các diễn đàn tự do cho việc mua bán các mẹo, các câu chuyện đùa và các thấu hiểu về cách các hệ thống khác nhau làm việc như thế nào - và trong một vài trường hợp có thể được làm để tiến hành những điều mà những người sáng tạo ra chúng không bao giờ có ý định. Đây là bản chất của việc vọc. Nó vốn dĩ không tốt cũng không xấu. Nó có thể là thứ này hoặc thứ kia, hoặc trong một số trường hợp là sự kết hợp của cả 2, phụ thuộc vào các động lực của các tin tặc.

Các thành viên của L0pht - danh sách chính xác thay đổi năm này qua năm khác nhưng trung bình là 7 hoặc 8 người - chia sẻ một sự mê hoặc với công nghệ và một sở trường cho việc kiểm thử các giới hạn của nó. Họ có thể giải mã chương trình chạy một mẩu phần cứng hoặc lặp đi lặp lại cơn lũ trường mật khẩu với quá nhiều ký tự, một lỗi được biết với cái tên "tràn bộ nhớ đệm" thường gây cho các hệ thống bị sập, mở cửa cho sự điều khiển tiếp sau.

"Sự khác biệt giữa cách nó giả định làm việc và cách nó thực sự làm việc là nơi mà các chỗ bị tổn thương xảy ra", Chris Wysopal, được biết như là Weld Pond trong những ngày ở L0pht của anh ta, nói.

Câu lạc bộ đầu tiên của nhóm - và sự truyền cảm hứng cho cái tên - từng là một gác xép thực sự trên một cửa hàng đồ gỗ ở ngoại ô South End Boston, được thuê sau khi bạn gái của một trong số các tin tặc trở nên mệt mỏi với tất cả các đồ đạt lủng củng lỉnh kỉnh các máy tính cũ làm bẩn căn hộ của họ (bao gồm cả vài mẩu được giữ lại bán thường xuyên trong phòng tắm của họ).

Giống như bản thân Internet, dường như có hiểm họa dưới và ngoài các con đường khắp xung quanh cái gác xép của L0pht trong kỷ nguyên trước chỉnh trang đô thị này. Nhưng bên trong từng là thiên đường của các lập trình viên, với các máy tính vứt khắp nơi, một cái TV, một chiếc đi văng, bia lạnh, và trò chơi đường mái vòm "Battlezone" những năm 1980 và một đường ray gây tò mò về những trang trí không bình thường cho người mẫu hàng dùng rồi, bao gồm cả xiêm áo, một mặt nạ chống hơi độc và một phần bộ quần áo cảnh sát mà các tin tặc đã tìm thấy. Trong một thỏa thuận may mắn, chủ nhà đã trả tiền điện mỗi tháng, giữ một đường dây điện bất tận chạy tới những gì được trang bị cho một phòng thí nghiệm máy tính khát điện.

"Từng là hoàn toàn đáng sợ để tới đó, nhưng một khi bạn ở đó rồi thì sẽ thích, 'Aha'", Joe Grand, một người nhiệt tình láu lỉnh và thích trượt ván, thành viên nhỏ tuổi nhất của L0pht, đã nhớ lại. "Đó thực sự là một nơi lẩn trốn theo nhiều cách. Nó thực sự đã định hình cuộc sống của tôi".

Nhiều đồ họ đã sử dụng - và cố nắn theo mong muốn của họ - từng được thu thập từ các bãi rác xung quanh khu công nghệ ở Boston. Các thành viên của L0pht đã tân trang vài phần cứng để bán ở các chợ trời để giúp trả tiền các hóa đơn, nhưng họ giữ lại các mẩu hữu dụng nhất, bao gồm cả một máy tính khổng lồ VAX - một khúc to của công nghệ cổ những năm 1970 với 2 chiếc, mỗi chiếc có kích thước của chiếc máy giặt - mà họ bằng cách nào đó đã đưa lên được cầu thang và vào trong gác xép.

Họ đặc biệt khinh thị những gì họ coi là an toàn theo danh sách kiểm tra, khi các công ty tuyên bố một sản phẩm an toàn chỉ vì họ đã triển khai một số chức năng tiêu chuẩn, như các mật khẩu và mật mã cơ bản. "Chúng tôi có thể nói, 'Hãy trao cho chúng tôi một cái. Chúng tôi sẽ thử phá nó'", Wysopal đã nhớ lại.

Họ hầu như đã luôn làm, thường là sau khi làm việc vất vả muộn vào buổi tối trong sự điên cuồng khám phá, tràn vào các hệ thống với các đầu vào mà các lập trình viên đã không biết trước hoặc theo bất kỳ cách gì được chuẩn bị. Paul Nash, tên tin tặc của anh ta là Silicosis, đã từng phát hiện ra là anh ta có thể phá các máy tính sử dụng các hệ điều hành Microsoft Windows phi trực tuyến bằng việc gửi một lệnh duy nhất - một mẹo mà anh ta hạnh phúc chỉ ra cho những khách tới thăm.

Khi các thành viên của L0pht đã không cố tìm các lỗi của riêng họ, thì

họ lại đang hỗ trợ cho những người khác trong việc làm thế, bao gồm qua những thu thập thường xuyên ở một quán rượu ở Boston trong đó bấy kỳ ai mà đã phát hiện ra một chỗ bị tổn thương mới của máy tính sẽ có được 3 cốc bia. L0pht cũng đã lan truyền về các phát hiện an toàn dù mạng tin của tin tặc (Hacker News Network), một nhóm tin phổ biến trên trực tuyến do Space Rogue quản lý, một thợ hàn lành nghề đã dựng lên cái đèn pin dùng tạm sao cho anh ta có thể đọc được trên giường ban đêm như một đứa trẻ. (Anh ta vẫn còn thường xuyên sử dụng tên tin tặc của anh ta hôm nay).

Mạng Tin của Tin tặc đã phát triển đủ phổ biến và nó đã cuốn hút sự quan tâm từ các địch thủ. Nhóm đã không muốn làm bẩn website chính của nó, L0pht.com, nhưng đã hạnh phúc để thu thập doanh thu từ Mạng Tin của Tin tặc. Một trong những quảng cáo sớm nhất được chào sẵn sàng, mất phí, là về các cô dâu Nga.

Video: Xem tài liệu gốc

Một nhóm các tin tặc đã tới Washington như thế nào.

Phơi các lỗi ra cho tất cả cùng thấy

L0pht một phần đã ôm lấy hình ảnh những đứa trẻ hư trong các tin tặc, tự gọi họ là "mũ xám", một khoảng đất nằm giữa sự có đức hạnh công khai các tin tặc "mũ trắng" và công khai ngoài vòng pháp luật các tin tặc "mũ đen". Nhóm đặc biệt thú vị trong việc thử để làm ngượng các công ty lớn, như Microsoft, vì bán các sản phẩm với các lỗi an toàn cho các khách hàng không có nghi ngờ gì.

Khi L0pht đã phát hiện ra cách để phá mật mã bảo vệ các mật khẩu của người sử dụng cho hệ điều hành Windows, Mudge đã công khai truy sát Microsoft vì những gì anh ta đã gọi là "mật mã nhà trẻ" và, cùng với Wysopal, đã tạo ra một công cụ phần mềm dễ dàng sử dụng để giúp bất kỳ ai khuất phục điều đó. Thành viên của L0pht Dildog đã phát triển một chương trình với nhóm tin tặc khác, gọi là Cult của Dead Cow, kiểm soát từ xa các mạng văn phòng chạy các phần mềm của Microsoft. Cái tên, một sự nhạo báng chương trình phổ biến của hãng "BackOffice Server 2000", từng là "Back Orifice 2000"; các tư liệu quảng cáo đặc trưng một biểu tượng thô thiển ngang bằng.

Nhưng thực tế L0pht từng theo quy ước hơn so với hình ảnh công khai. Wysopal từng là một lập trình viên cho Lotus. Space Rogue và 2 người khác đã làm việc ở CompUSA, một chuỗi cửa hàng. Vài người đã có công ăn việc làm ở BBN Technologies, một công ty công nghệ đáng tôn kính nhiều năm trước đã giúp xây dựng người tiền nhiệm

quan trọng của Internet, một dự án do Lầu 5 góc tài trợ gọi là ARPANET.

Mọi người đã sử dụng các cái tên tin tặc của họ chủ yếu vì họ sợ bị đánh nếu các ông chủ của họ biết được các hoạt động về đêm của họ. (Lý do khác, cũng quan trọng, là họ muốn làm cho khó khăn hơn đối với các công ty đối mặt với sự lúng túng khi muốn kiện họ hoặc gọi cảnh sát - các mối đe dọa có thực, lúc này lúc khác, cho bất kỳ ai tiến hành nghiên cứu tự do về an toàn).



Các tin tặc "Mũ đen / Mũ trắng"

Những người khai thác các lỗi trong các hệ thống máy tính. Các chuyên gia an toàn tìm cách tìm ra và sửa các lỗi thường tự gọi họ là các tin tặc "mũ trắng". Các tin tặc tội phạm hoặc độc hại được gọi là "mũ đen".

Các công ăn việc làm ban ngày cũng đưa ra một cái nhìn của người trong cuộc về nền công nghiệp công nghệ đang bùng nổ, giúp các tin tặc thấy được các lỗi trong kinh doanh hoặc các sản phẩm tiêu dùng được sử dụng rộng rãi. Các công ty mà dường như không có trách nhiệm về các kêu ca qua các kênh chính thống tự thấy bản thân họ trong tầm ngắm của L0pht. Nhóm đó đã duy trì các đường dây mở tới vô số các tin tặc khác - bao gồm cả các tin tặc làm việc bên trong các hãng công nghệ lớn - và đã phát triển sự khinh thị đối với văn hóa kinh doanh mà họ nói đặt lợi nhuận lên trên sự an toàn.

"Điều đó là có triển vọng, làm cho mọi điều chạy nhanh như chúng ta muốn. Hãy kiếm ít tiền", Nash nói. "có sự thúc đẩy khổng lồ để có được mã ở bên ngoài, và chúng ta sẽ sửa nó sau".

L0pth cũng nghi ngờ sự hăng hái của các công ty sửa các lỗi thậm chí sau khi họ đã phát hiện. Trong những năm đầu của nhóm, các báo cáo tới các địa chỉ thư điện tử chính thức của công ty - đã thiết lập có chủ đích để thu hút sự quan tâm về an toàn - dường như thường chỉ biến mất vào lỗ đen. Một kẻ tội phạm đặc biệt, các thành viên L0pht nói, là secure@microsoft.com.

Họ cuối cùng đã phát hiện ra một cách thức tin cậy để kéo sự chú ý của các công ty: Các cảnh báo an toàn được đưa lên L0pht.com đã lôi kéo sự chú ý từ các nhà báo công nghệ trên thế giới và cuối cùng bản thân các công ty đó.

Mặt trái là nhiều tin tặc "mũ đen" cũng đã giám sát các cảnh báo của L0pht, trao cho họ thời gian để tận dụng các lỗi trước khi các công ty có thể có khả năng sửa chúng. Không có cách gì biết làm thế nào nhiều chỉ dẫn điều này đã giúp, nhưng các thành viên của L0pht đã không biện giải.

"Chúng tôi luôn nghĩ rằng nếu chúng tôi biết về nó, thì những người khác cũng có thể biết về nó và đang khai thác nó", Grand, được biết

tới như là Kingpin, nói.

Bill Gates cưỡi 'thủy triều'

Năm 1993 tới với trình duyệt web phổ biến rộng rãi nhất, Mosaic, đã làm cho Internet trở thành một sức mạnh thương mại và văn hóa không thể dừng lại được. Bỗng nhiên nó đã không là miền đất hứa đẹp đẽ kỳ lạ cho người giỏi kỹ thuật. Bất kỳ ai cũng có thể "lướt Web".

Vài năm tiếp sau, các ngôn ngữ lập trình mới và phức tạp như Flash và Java đã mở rộng đột ngột các khả năng của trình duyệt. Các website đã bắt đầu có các video. Các trò chơi như "Frogger," "Super Mario Bros." và "Tetris" có thể chơi được, tự do không mất tiền, trên bất kỳ máy tính nào mà có thể lên trực tuyến được.

Đối với hầu hết những người sử dụng, các tính năng mới dường như hầu hết là ma thuật. Chúng dường như tự động, có lẽ đòi hỏi chỉ 1 hoặc 2 cái nháy chuột. Sớm, hầu hết các máy tính trên thế giới đã có Flash và các ngôn ngữ lập trình tương tự trong các ổ đĩa cứng của họ.

Sự quan tâm của những người tiêu dùng đang nổi lên từng không phải là sự mất mát ở phía của người đồng sáng lập ra Microsoft, Bill Gates, người đã gửi một ghi chép bí mật cho các lãnh đạo hàng đầu của ông vào tháng 05/1995 với đầu đề "Cơn thủy triều Internet". 5.500 tài liệu văn bản được yêu cầu trong việc quét, những khoản cấp bách mà công ty cạnh tranh mạnh mẽ trong thị trường trực tuyến mới bùng nổ đó.

"Ít năm nữa sẽ là rất thú vị khi chúng ta xử trí các thách thức và cơ hội đó", Gates viết. "Internet là một cơn thủy triều. Nó thay đổi các quy tắc. Nó là một cơ hội không thể tin được cũng như thách thức không thể tin được. Tôi nhìn về phía trước cho đầu vào của bạn về cách mà chúng ta có thể cải thiện chiến lược của chúng ta để tiếp tục ghi dấu thành công không thể tin được của chúng ta".

Gates đã cảnh báo về tầm quan trọng về an toàn trong ghi chép đó, nói "Các kế hoạch của chúng ta về an toàn cần phải được tăng cường". Nhưng ông ta cũng nói, "Tôi muốn mọi kế hoạch sản phẩm để thử và đi vượt khỏi các tính năng của Internet".

Ưu tiên này, nhiều chỉ trích có thể nói sau này, từng là ưu tiên quan trọng nhất cho Microsoft, gieo hạt những gì mà các chuyên gia an toàn đã gọi là "featuritis" - một căn bệnh phổ biến trong đó các tính năng mới được bổ sung nhanh hơn so với việc chúng có thể được làm cho

Ảnh trái: Xem tài liệu gốc

Các thành viên của L0pht, bao gồm, từ trái qua, Tan, Kingpin, Weld Pond, Mudge và Brian Oblivion, đã thuê một chiếc xe tải cho chuyến đi của họ tới Washington để làm chứng ở Thượng viện vào tháng 05/1998.

Ảnh phải: Xem tài liệu gốc

Các tin tặc bên ngoài khách sạn của họ vào buổi sáng làm chứng của họ: từ trái qua, Kingpin, Brian Oblivion, Weld Pond, Tan, Mudge (quỳ gối), Space Rogue and Stefan von Neumann.

an toàn.

Sự vội vã sáng tạo này, làm cho mọi sản phẩm của Microsoft về cơ bản là một sản phẩm Internet, đã cảm nhận được sâu sắc khắp công ty, Billy Brackenridge, một quản lý chương trình của Microsoft trong những năm 1990, nói. Khả năng phân phối các tính năng mới cho các hệ điều hành cồng kềnh và phần mềm của công ty đã xác định ai có được các lựa chọn cổ phiếu - một động lực chính cho công ty mà cổ phiếu chia 7 lần thập kỷ đó trong khi tổng thu hơn 9.000%.

“Có lẽ có 1 hoặc 2 người thực sự quan tâm [tới an toàn]. Phần lớn, từng là, 'Hãy đưa nó ra cửa'”, Brackenridge đã nhớ lại. “Nếu chúng ta ra muộn, đó là tiền thật... Nếu tính năng của bạn đã không có, thì bạn sẽ không có cổ phần”.

Các tinh túy cạnh tranh của Microsoft đã khuyến khích sức đẩy điên cuồng để phát triển một trình duyệt để thách thức người dẫn đầu Netscape Navigator, nó từng được sản xuất phần lớn từ đội các lập trình viên y hệt, những người đã tạo ra Mosaic. Vào giữa những năm 1990, Navigator đã có hơn 70% thị phần, Gates đã cảnh báo trong bản ghi chép của ông ta.

Câu trả lời của Microsoft là tạo ra Internet Explorer và tích hợp trình duyệt đó mạnh mẽ vào với hệ điều hành Windows áp đảo của hãng. Nỗ lực này là trọng tâm đối với tố cáo chống cạnh tranh của Bộ Tư pháp chống lại Microsoft, điều đã được thiết lập vào năm 2001.

Nhưng nó đã có các tác động khác đáng chú ý ngay lập tức đối với L0pht và các tin tặc khác.

Khi Microsoft đã làm việc để đưa các tính năng có liên quan tới Internet vào các sản phẩm của hãng, hãng đã tạo ra các cổng cho các tin tặc để phát hiện và khai thác. Một cổng đặc biệt rõ ràng từng là một ngôn ngữ lập trình gọi là ActiveX, điều giống như Flash và Java đã đạt được sâu trong tâm trí của máy tính một người sử dụng.

“Một khi bạn đi tới một website và tải về vài mã và nó tự chạy... thì bạn có kiểu vấn đề hoàn toàn mới”, Giovanni Vigna, một nhà khoa học máy tính ở Đại học California ở Santa Barbara và là đồng sáng lập ra Lastline, một công ty về an toàn, nói. “Bây giờ tôi có mã chạy được trên máy tính của bạn, và tôi có thể làm bất kỳ điều gì thú vị”.



Trình duyệt

Chương trình cho phép mọi người truy cập tới Web. Các trình duyệt kéo thông tin từ một loạt các máy chủ khắp Internet và có thể làm lộ những người sử dụng đối với các rủi ro về an toàn.

Ảnh: Xem tài liệu gốc

Cris Thomas, tên hiệu là Space Rogue, đã có một công việc ban ngày ở CompUSA khi anh ta từng là một thành viên của L0pht. (Bill O'Leary của The Washington Post).

700 người sử dụng, 1 mật khẩu ngu ngốc

Tại một hội nghị các tin tặc vào tháng 08/1997, Mudge - tên thật là Peiter Zatko và là người đã truyền nhiệt huyết cho tinh thần tự đề cao sản phẩm của mình trong L0pht - đã hài lòng ra mặt trong việc vọc Microsoft khi anh ta đã mô tả việc phá an toàn mật khẩu trong Windows, vào thời điểm hệ điều hành tiêu chuẩn đó được dùng cho các máy tính của doanh nghiệp và chính phủ khắp thế giới.

"Tôi đã không muốn làm việc trên các sản phẩm của Microsoft ngay bây giờ", Mudge nói. "Vấn đề là: Chúng là ở khắp mọi nơi! Bạn không thể thoát ra khỏi chúng!".

Anh ta đã một mình đưa ra lỗi an toàn đặc biệt quá xá - chia một trường mật khẩu 14 ký tự thành 2 mật khẩu 7 ký tự yếu hơn nhiều để lưu trữ. Mật khẩu càng dài, thì tin tặc càng phải thử chia nó thành nhiều sự kết hợp hơn. Nhưng Microsoft, Mudge đã nêu, đã làm xói mòn nguyên tắc đó bằng việc tạo, về cơ bản, 2 mật khẩu ngắn hơn và dễ phá hơn thay vì một mật khẩu mạnh.

Tệ hơn, nếu người sử dụng đã chọn một mật khẩu từng là 7 ký tự hoặc ít hơn, thì hệ thống lưu giữ một chuỗi các ký tự mách lẻo để trình bày phần không được sử dụng của trường mật khẩu đó. Khi các tin tặc thấy chuỗi này, họ biết rằng họ đã phá được nửa mật khẩu. Mudge hạnh phúc kể lại sự kết hợp kỳ cục các ký tự và con số ở hội nghị, với hàng tá các tin tặc nhìn vào.

"Tôi sẽ xăm lên trán và đi khắp các phòng của Microsoft!" anh ta đã nói trong tiếng cười của đám đông.

Anh ta cũng đã tuyên bố rằng L0pht đã phát hiện ra rằng một mật khẩu duy nhất - "CHANGEME" - đang được 700 người sử dụng dùng trong một mạng mà nhóm đã nghiên cứu.

Những trò cười như vậy đã lôi cuốn các fan hâm mộ trong thế giới các tin tặc, một ngụ ý bóng gió về sự nổi tiếng rộng hơn và luồng tiền đầu tiên sẽ tới. L0pht đã bán các áo T-shirt có logo của mình ở các hội nghị và cũng bắt đầu bán công cụ của mình để phá các mật khẩu Windows - gọi là L0pht Crack - với giá 50 USD cho các quản trị hệ thống thích thử độ dài các mật khẩu trong các mạng mà họ đã quản lý.

Khi các thành viên của L0pht đã biết được có nhiều nhà tư vấn về an toàn đã lấy tiền cho các dịch vụ như vậy, thì họ đã nâng giá lên 150 USD, rồi 500 USD. (Một trong những người mua là Văn phòng Kiểm

toán Chính phủ - GAO [Government Accountability Office], một cơ quan giám sát của liên bang mà ghi chép các thất bại của các hệ thống CNTT liên bang).

Đối với tất cả thú săn đuổi của L0pht để phá các hệ thống trực tuyến, các thành viên đã từ lâu quản lý câu lạc bộ của họ với một thủ tục nhất định. Họ đã có các cuộc họp thường xuyên, thiết lập các ưu tiên thu thập và điều khiển các vấn đề tài chính một cách cẩn trọng. Từng tin tặc đã có các bàn làm việc riêng của mình và trả 100 USD mỗi tháng tiền thuê trước; những ai không thể kham được điều đó có thể chia sẻ các bàn làm việc và trả nửa số tiền.

Nhưng việc vội vã kiếm tiền trong an toàn máy tính đã gây ra sự chú ý vào chúng. Họ có một cảm tưởng đầu tiên về nó khi các quảng cáo trực tuyến bán các áo T-shirt và L0pht Crack có nghĩa là các thành viên không còn phải móc sâu vào túy của riêng họ để trả tiền thuê nhà hoặc các chi phí khác. Họ cũng đã lưu ý thấy cách mà một thế hệ các nhà tư vấn về an toàn đang nảy sinh - bao gồm cả một vài nhóm làm "các kiểm thử cố gắng" bằng việc sử dụng các chiến thuật rất giống với L0pht - đã có được những ngày được trả tiền.

Vào lúc L0pht xuất hiện trước Thượng viện vào năm 1998, ý tưởng về bắt đầu một công ty thực sự - và kiếm đủ lợi nhuận để bỏ các công việc hàng ngày của họ - từng bắt đầu hình thành bên trong nhóm.

"Bạn biết đấy", Space Rogue đã nhớ lại, "có lẽ chúng ta nên có một mẩu về điều đó".

Đây là sự khởi đầu và là sự kết thúc đối với L0pht.

Ảnh trái: Xem tài liệu gốc

Joe Grand, tên hiệu là Kingpin, vào năm 1996, sử dụng một radio để nhận đánh số trang và các cuộc truyền máy đầu cuối dữ liệu di động của cảnh sát. (Courtesy of Joe Grand).

Cuộc gọi gần ở NSA

Họ đã có một cuộc du ngoạn ồn ào tới Washington để làm chứng trước Thượng viện, thuê một chiếc xe tải xanh sẫm, 15 chỗ ngồi và cài đặt dãy các ăng ten trên nóc để xem các tín hiệu họ có thể bắt trên đường.

Ảnh phải: Xem tài liệu gốc

Một gác xép một cửa hàng đồ mộc ở ngoại vi South End của Boston đã cung cấp cảm hứng cho cái tên L0pht. Nhiều phần cứng máy tính trong môi trường đó đã được quét tìm từ các khu thùng rác ở Boston. (Courtesy of Joe Grand)

Điều này dường như giống như trò vui của các tin tặc vô hại cho tới khi họ dừng ở Bảo tàng Mật mã Quốc gia, trên nền của Cơ quan An ninh Quốc gia (NSA) ở ngoại ô Maryland. Zatko đã tới thăm NSA vài lần trước đó, anh ta nói, một phần của sự chuyển dần vào trong công việc của chính phủ liên bang. "Tôi đã muốn họ có được sự nhạy cảm, để biết rằng các tin tặc không phải là những người xấu", anh ta đã giải thích sau đó.

Nhưng trong chuyến đi này, Zatko ngẫu nhiên hướng dẫn chiếc xe tải của L0pht, nóc của nó dựng đứng với các thiết bị giao nhau, tới lối vào của một khu an toàn của khu vực NSA. Lái chiếc xe từng là thành viên của L0pht Stefan von Neumann, người dường như đã lúng túng khi anh ta lái xe tới một điểm kiểm soát có lính gác có vũ trang. Khi người lính chào von Neumann, tên thật của anh ta là Stefan Wuensch, thì anh ta đã hỏi các tin tặc bạn của anh ta, "Tôi nên làm gì?"

Cùng đồng thanh, họ đã hét lên, "Chào lại!"

Nhưng một khi nằm trên đất của cơ quan gián điệp bí mật nổi tiếng đó, thì các thành viên của L0pht nhanh chóng thấy không dễ và thúc giục von Neumann thoát ra khỏi khu đất đó càng nhanh càng tốt. Anh ta đã sớm làm thế, đưa chiếc xe tới viện bảo tàng, rồi tiến về Washington mà không có sự cố nào nữa.

Các tin tặc đã làm chứng vào ngày hôm sau trước Ủy ban các Công việc Chính phủ của Thượng viện (Senate Governmental Affairs Committee), các nhân viên của Ủy ban đã nói cho L0pht rằng chỉ các thành viên của các chương trình bảo vệ nhân chứng liên bang trước đó được phép làm chứng bằng việc sử dụng các tên hiệu. Các tin tặc sau đó đi một tua dạo Nhà Trắng, được quan chức chống khủng bố của Hội đồng An ninh Quốc gia (National Security Council) Richard A. Clarke dẫn đi.

Câu chuyện trang bìa trên tạp chí Internet Week (Tuần Internet), kể về Wysopal và Zatko (là Weld Pond và Mudge), cuối cùng đã thổi bay bức màn che của họ ở nơi làm việc, nhưng họ đã không bị sa thải như họ từng sợ. Tạp chí New York Times cũng đăng câu chuyện của L0pht, giống như PBS và MTV đã làm. Những khoác lác về các tin tặc đang có khả năng đánh sập Internet trong vòng 30 phút - bằng việc khai thác các lỗi trong giao thức định tuyến Internet chủ chốt gọi là BGP - đã được nhắc tới từ Conan O'Brien và Rush Limbaugh, những người đã gọi chúng là "các tin tặc máy tính mọt sách tóc còn xanh".

Thậm chí các nhà sản xuất của Trivia Pursuit cũng đã để ý tới. Câu hỏi: Nhóm các cao thủ gọi là L0pht đã nói cho Thượng viện Mỹ họ có thể đánh sập Internet trong vòng 30 phút?

Câu trả lời: Internet

Vào thời điểm mà xuất bản trò chơi chiếm chỗ trong các cửa hàng vào năm 2000, L0pht không còn là L0pht nữa. Các tin tặc đã ra nhập @Stake, một công ty về an toàn được xây dựng phần lớn dựa vào

khung của L0pht và 10 triệu USD vốn đầu tư rủi ro. Họ đã bỏ công việc hàng ngày của họ và cuối cùng đi theo thú vui về đêm của họ toàn thời gian.

Nhưng họ cũng đã có được một tập hợp các quy tắc và trách nhiệm mới không quen thuộc - đặc biệt cho các khách hàng mà đã hạnh phúc trả tiền vì sự tinh thông của họ nhưng đã không thích bị nướng công khai bất kỳ khi nào các tin tặc phát hiện ra các vấn đề.

“Cộng đồng chúng tôi tới từ đó đã nghĩ chúng tôi đã bán sạch, điều tất nhiên chúng tôi đã làm, Wysopal nhớ lại”.

Trong số các công ty lớn nhất thuê @Stake - và yêu cầu các thỏa thuận kín về những gì họ thấy - là nữ thần báo ứng lâu đời của L0pht: Microsoft.

Hạ chiếc rìu

Khi các thực tế kinh doanh được đặt ra, Space Rogue từng là nạn nhân đầu tiên. Anh ta đã quản lý các hoạt động bên lề của L0pht và cũng của Hacker News Network. Nhưng các nhà đầu tư rủi ro đã có những người vận hành của riêng họ, và họ đã không thiết tha về việc lập nhánh công khai cho bản thân họ với từ “tin tặc”.

Nên nhóm tin trực tuyến đã trở thành website tập đoàn được làm sạch gọi là “Security News Network” (Mạng Tin tức về An toàn), và Space Rogue có một công việc ở phòng tiếp thị của @Stake - xa với trung tâm hấp dẫn nơi mà Mudge, Kingpin, Weld Pond và những người khác đã làm việc. Space Rogue đã sớm bị sa thải sau đó.

Công ty đã tịch thu máy tính cá nhân của anh ta và đã hộ tống không cần nghi thức anh ta ra khỏi cửa vì các lý do anh ta nói anh ta vẫn không hiểu. Vào thời điểm Space Rogue về nhà, các tài khoản của anh ta trên L0pht.com đã bị loại bỏ. Anh ta đã không biết - và bây giờ vẫn không biết - liệu có bất kỳ ai trong số các tin tặc bạn anh ta đã nói hộ cho anh ta hay đã chiến đấu chống lại sự sa thải đó hay không.

“Điều đó từng là một phần tồi tệ trong cuộc đời tôi... Tôi mất 6 người bạn tốt nhất”, Space Rogue nhớ lại. “Nó thực sự phá hủy tôi. Nó làm tôi mất nhiều thời gian để phục hồi từ đó”.

Bong bóng dot-com, điều đã đẩy các giá trị các công ty công nghệ vào tầng bình lưu, bùng phát vào khoảng thời gian đó, quét sạch các công ty yếu như Pets.com và thất doanh thu khắp nền công nghiệp. Giám

Ảnh: Xem tài liệu gốc

Chris Wysopal, còn được biết tới như là Weld Pond trong những ngày ở nhóm L0pht của anh ta, đứng trước máy chiếu trang chủ Web của nhóm. Wysopal và một người bạn tin tặc ở L0pht, Dildog, đã thành lập công ty về an toàn Veracode vào năm 2006. (Bill O'Leary / The Washington Post).

đốc điều hành của @Stake, người từng được mang tới để cung cấp thứ gì đó giống như giám sát của cha mẹ đối với L0pht, đã ra lệnh cho Wysopal chọn ra một thành viên của nhóm để sa thải để cân bằng với sự cắt giảm khắp nơi trong công ty.

Wyposal nói anh ta đã miễn cưỡng hạ cái rùi vào Brian Oblivion, một trong những thành viên cá tính của L0pht, tên thật của anh ta là Brian Hassick. Sự sa thải tới vào ngày trước khi con trai của Hassick được đặt tên rửa tội; anh ta và Wysopal đã không nói lại nhiều tháng.

Khi các mối quan hệ ở trong tim của L0pht đã hỏng, Zatko đã biến mất một cách huyền bí. Dù không phải thành viên sáng lập nhóm, anh ta từng là bộ mặt công khai nhất của nó khi danh tiếng nổi lên.

Nếu L0pht từng là thứ gì đó giống như ban nhạc nổi tiếng Beatles của thế giới các tin tặc - kết hợp các cái miệng nghiêm túc với một bản năng tự quảng cáo - thì Zatko từng là người lanh lợi, dạng người như John Lennon, còn Wysopal giống như Paul McCartney vậy.

Nhưng khi @Stake đang vật lộn với khó khăn, thì Zatko đã phát triển mối bận tâm gay gắt, làm cho tệ hơn bằng một phản ứng tồi tệ với thuốc mà từng được hỗ trợ để giảm nhẹ các triệu chứng, anh nói. Zatko đã dừng lại trong một bệnh viện tâm thần trong vài ngày. Không ai trong số các thành viên của L0pht tới thăm, một nguồn thất vọng bất tận cho anh ta. (Họ nói họ đã không biết điều gì đã xảy ra, chỉ biết rằng anh ta đã biến mất khỏi công việc).

“L0pht từng là gia đình duy nhất của tôi”, Zatko đã nhớ lại. “Nó đã giết tôi... Điều thực sự tàn bạo”.

Dù Zatko dần phục hồi, thì sự đi xuống của @Stake vẫn tiếp tục. Space Rogue đã đe dọa một vụ kiện đòi lại lương đã mất và cổ phần còn lại của anh ta trong việc cấp vốn đầu tư rủi ro ban đầu. (Anh ta cuối cùng đã dàn xếp được với tiền đủ mua một chiếc ô tô, trả được phí luật sư và đưa sự thanh toán về chế độ công quản, anh ta nói).

Có lẽ điểm còn thậm chí thấp hơn cho @Stake tới vào tháng 09/2003, khi công ty đã sa thải giám đốc công nghệ của nó, cao thủ về an toàn được tôn trọng như Dan Geer, sau khi ông là đồng tác giả một nghiên cứu về cách mà sự áp đảo của Microsoft trong nền công nghiệp phần mềm đã làm xói mòn an toàn. Geer đã biết về sự sa thải của anh ta qua một tin phát hành của @Stake, theo các báo cáo tin tức vào lúc đó.

Khi Symantec, một hãng về an toàn lớn hơn, đã mua phần còn lại của

@Stake vào năm 2004, nó từng là một sự giết chết có hàm ơn.

“Mọi điều chúng tôi biết là nó đã bị rỉa từng chút một cho tới khi chúng tôi chẳng còn lại gì”, Grand nói. “Chúng tôi cần phải có khả năng nói lên sự thật về mọi người. Điều đó đã không kéo dài mãi... Cuối cùng chúng tôi chỉ đứng được bằng đầu gối của chúng tôi trước mọi người”.

Khi L0pht đã sụp đổ, an toàn trên Internet đã trở nên còn tồi tệ hơn. Những ngày cảnh báo những đầu tư khổng lồ đặc trưng của thế kỷ 20 hướng vào việc sửa lỗi Y2K - dựa vào cảnh báo khả năng là các chương trình được thiết kế để nhận các năm bằng chỉ 2 ký tự số, như “99”, có thể bỗng nhiên sụp đổ khi chúng thấy “00”.

Nhưng các vấn đề có thể sớm làm điêu đứng điện toán đã không ngẫu nhiên, giống như lỗi Y2K. Các tin tặc mũ đen đã gia tăng.

Trong số những thảm họa về an toàn đầu tiên của thập niên tiếp sau, sâu ILOVEYOU, đã tới vào tháng 05/2000 và hình như từng là công việc của 2 lập trình viên máy tính từ Philippines.

Virus đó đã khai thác một tính năng trong Microsoft Outlook và gửi mã độc đó tới từng liên hệ của nạn nhân mới trong các danh sách thư.

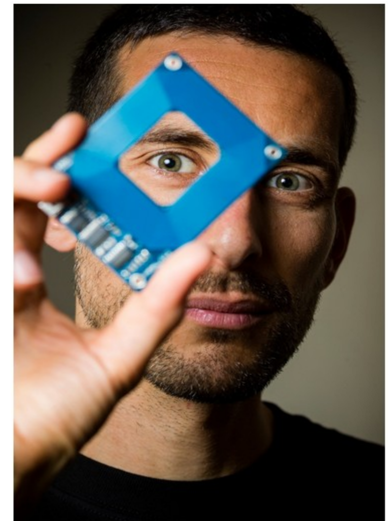
Sớm, ước tính 10% các máy tính trên thế giới đã bị lây nhiễm, gặm nhấm các mạng của Lầu 5 góc, Quốc hội Anh và nhiều công ty tư nhân. Ước tính thiệt hại và chi phí làm sạch khoảng 20 tỷ USD. Nhiều sâu khác - với các cái tên như Pikachu, Anna Kournikova và Nimda — cũng đã khai thác các lỗi trong các sản phẩm của Microsoft.

Vào ngày 08/12/2000, một ngày trước lễ kỷ niệm cuộc tấn công đáng kinh ngạc của Nhật Bản vào các lực lượng hải quân Mỹ vào năm 1941, Clarke - quan chức của Hội đồng An toàn Quốc gia, người đã từng trao cho L0pht một tua đi thăm Nhà Trắng - đã xuất hiện ở một hội nghị được Microsoft tổ chức. Ông đã cảnh báo rằng nếu chính phủ không cải thiện an toàn máy tính, thì quốc gia có thể chịu một “trận Chân Châu Cảng số”.

'Các tin tặc giống như nước'

Di sản của L0pht là một di sản pha trộn. Nhóm từng trong số những người tiên phong của một hệ thống gọi là “mở có trách nhiệm”, vẫn được sử dụng rộng rãi ngày nay, trong đó các nhà nghiên cứu mà tìm thấy các lỗi sẽ trao cho các công ty một thiết lập lượng thời gian để

sửa lỗi trước khi các lỗi về an toàn đó được công bố cho thế giới. Vài công ty bây giờ đã bước tiếp, chào các phần thưởng bằng tiền mặt được gọi là "tiền thưởng vì các lỗi" (bug bounties) để khuyến khích các tin tặc tìm kiếm các vấn đề - và lý tưởng tìm chúng trước các tội phạm và gián điệp.



Ảnh: Xem tài liệu gốc

Joe Grand, người trước đó đã sử dụng tên tin tặc Kingpin, ở nhà của anh ta ở Portland, Ore., với một đầu đọc thẻ RFID anh ta đã thiết kế. (Leah Nash cho tờ The Washington Post)

Microsoft cuối cùng đã trở nên nghiêm túc hơn về an toàn. Nó đã không có nhiều sự lựa chọn: Các khách hàng chính đã nói cho Gates hoặc làm tốt hơn hoặc đánh mất việc kinh doanh của họ. Trong một ghi chép vào tháng 01/2002 - thứ gì đó của một bookend cho ghi chép từ 1995 - Gates đã nói rằng một sáng kiến mới về an toàn là "ưu tiên cao nhất cho tất cả công việc chúng ta đang làm".

Động thái ban đầu đó đã lôi kéo vài sự hoài nghi. "Khi tôi đã nói cho các bạn rằng tôi từng tới Microsoft để làm việc về an toàn... hầu hết họ cười vào mặt tôi vì tôi đã sử dụng các từ 'Microsoft ' và 'an toàn' trong cùng một câu", Scott Charney, một quan chức Bộ Tư pháp được thuê vào năm 2002, nói. Ông bây giờ là phó chủ tịch tập đoàn về Điện toán Tin cậy ở Microsoft.

Microsoft đã rút ra hàng ngàn kỹ sư khỏi phát triển sản phẩm để đại tu các hệ thống của công ty cho việc thiết kế và xây dựng phần mềm. Gates gửi một nhóm các quan chức tới một nơi ẩn dật trong một ngôi nhà gỗ lịch sử thường được sử dụng cho các đám cưới, gần Bellevue, Washington, khoảng 15 phút lái ô tô từ tổng hành dinh của Microsoft ở Redmond. Charney nói, "Về cơ bản vài người được gửi tới đó và nói, đừng quay lại cho tới khi bạn có được câu trả lời".

Nhưng Internet đã không bỗng nhiên trở nên an toàn. Trọng tâm mới thấy của hãng về an toàn đã mất nhiều năm để hái quả, hầu hết đáng chú ý với sự ra đời của Windows Vista vào năm 2006 và Office 2010 ít năm sau đó. Vì nhu cầu cho "tính tương thích ngược" - nghĩa là các phiên bản cũ hơn và mới hơn các sản phẩm của Microsoft làm việc dễ dàng với nhau - các lỗi cũ chậm trễ trong thế giới trực tuyến nhiều năm sau họ đã sửa trong phần mềm mới được phát hành.

Chính phủ liên bang trong năm ngoái cuối cùng đã thay thế hàng trăm ngàn máy tính chạy Windows XP - hệ điều hành lần đầu được phát hành vào năm 2001, vài tháng trước khi Gates kêu gọi trang bị an toàn sản phẩm - sau khi công ty đã rút khỏi sự hỗ trợ tự do gần 13 năm.

Khi các sản phẩm của Microsoft đã trở nên an toàn hơn, các tin tặc đã bắt đầu ăn cỗ trên các mục tiêu lựa chọn thay thế mà đã không có

được sự đại tu tương tự.

“Các tin tặc giống như nước”, Vigna, nhà khoa học máy tính ở Đại học California ở Santa Barbara, nói. “Họ luôn đi vào con đường ít có sự kháng cự nhất... Nếu bạn đặt một cài cắm đúng chỗ, họ sẽ tìm thấy vết nứt khác”.

Trong gốc rễ là một vấn đề được L0pht đã nêu khi làm chứng trước Thượng viện: Các khuyến khích kinh doanh trong nền công nghiệp kỹ thuật công nghệ có lợi cho sự tăng trưởng hơn là an toàn. Và một khi các công ty đủ lớn và an toàn là một lo ngại chính - như cuối cùng đã xảy ra với Microsoft - là cực kỳ khó để trang bị mới các bảo vệ chặt chẽ trong các hệ thống được xây dựng mà không có chúng.

Thompson, người của đảng Cộng hòa bang Tennessee, người làm chủ tịch nhóm Thượng viện vào năm 1998 và đã rời bỏ Quốc hội vào năm 2003, nói trong một cuộc phỏng vấn gần đây rằng an toàn của Internet là dạng vấn đề mà chính phủ có lo ngại sửa. “Số 1, nó là rất khó, và số 2, không có tiền chi trả về chính trị cho bất kỳ ai”.

Sự nổi lên của các tin tặc mũ đen

Vì nhà bình luận của giới công nghiệp thích các tiêu chuẩn khắt khe của chính phủ và trách nhiệm giải trình pháp lý đối với những thất bại, như từ lâu đã tồn tại nhiều hệ thống sống còn phi trực tuyến như các ô tô, thang máy và máy bay. Những người khác có thể tạo ra một nhóm độc lập, một nền công nghiệp kỹ thuật cho các Phòng thí nghiệm của những người bảo kê, chúng chứng thực sự an toàn của các thiết bị điện tử trên thế giới. Hoặc có lẽ các công ty bảo hiểm, chúng cuối cùng đền bù thanh toán hóa đơn cho nhiều sự cố an toàn không gian mạng, có thể một ngày nào đó yêu cầu các thực tiễn an toàn tốt hơn từ các khách hàng của họ, như những người bảo hiểm đã làm cho các ngôi nhà và ô tô của họ.

Nhưng những người khác đã viện lý rằng các đòi hỏi về an toàn tốt hơn có thể cản trở đổi mới và làm cho các sản phẩm công nghệ khó sử dụng. Biết rằng vai trò trung tâm ngày càng gia tăng của nền công nghiệp này trong kinh tế quốc gia - và sự mở rộng khổng lồ trong sức mạnh vận động hành lang ở Washington những năm gần đây - thì pháp luật hoặc quy định mới gay gắt vẫn khó để tưởng tượng.

“Cách duy nhất để lôi ra trước mặt vấn đề về an toàn là xây dựng các

Ảnh: Xem tài liệu gốc

Paul Nash, tên hiệu là Silicosis, bên trái, và Chris Wysopal, tên hiệu là Weld Pond. Các thành viên của L0pht cuối cùng đã bỏ các công ăn việc làm ban ngày để ra nhập @Stake, một công ty về an toàn. “Cộng đồng mà từ đó chúng tôi đã tới đã nghĩ chúng tôi từng bán sạch, điều tất nhiên chúng tôi đã làm”, Wysopal nói. (Bill O'Leary / The Washington Post).

phần mềm tốt hơn”, Gary McGraw, giám đốc công nghệ cho Cigital, một hãng có trụ sở ở Northern Virginia từng làm việc về an toàn phần mềm từ những năm 1990, nói. “Chừng nào chúng ta còn chưa bắt đầu xây dựng được an toàn, chừng đó chúng ta còn chơi trò đuổi bắt”.

Bản thân L0pht đã làm bật lên được một chút, phát hành một phiên bản được cập nhật của L0pht Crack vào năm 2009. Website chính vẫn còn chạy, nếu một ít ngày tìm kiếm. Mạng Tin của Tin tặc đã giành lại được tên của nó và góc cạnh của nó.

Wysopal và người bạn tin tặc ở L0pht Dildog đã thành lập một công ty về an toàn, Veracode, vào năm 2006. Zatko, sau khi phục hồi từ lo âu nặng nề, đã ra nhập lại BBN Technologies. Anh ta sau đó đã trải qua 3 năm chỉ đạo nghiên cứu về an toàn không gian mạng ở Cơ quan các Dự án Nghiên cứu Tiên tiến của Quân đội (DARPA), cơ quan của Lầu 5 góc mà đã tạo ra mạng tiền thân của Internet vài thập kỷ sau đó, trước khi trở thành phó giám đốc cho một đội nghiên cứu ở Google.

Hầu hết những người khác vẫn còn làm việc trong lĩnh vực an toàn máy tính. Họ đã có sự tái ngộ các dạng khác nhau vào mùa hè 2014 trong đám cưới của Space Rogue ở Philadelphia. Các vết thương lòng từ sự sụp đổ của @Stake đã lành sẹo nếu không nói là đã biến mất.

Còn đối với các vấn đề an toàn họ từng nhấn mạnh cho chính phủ Mỹ và thế giới, tin tức là tệ hơn nhiều. Các tin tặc - dạng mũ đen - đã luôn chạy quá các nỗ lực để áp đặt sự an toàn.

Wysopal đã đưa ra tiền lệ dữ dằn này: Các thành phố từng bị tổn thương vì các vụ cháy thảm họa, điều đã dữ dội qua các đám chật chội các tòa nhà được xây dựng hầu hết bằng gỗ. Đã có vụ cháy khổng lồ ở Chicago để thúc các quan chức chính phủ trong các cải cách nghiêm túc, bao gồm cả các hạn chế xây dựng mới bằng gỗ, một hệ thống cung cấp nước mạnh mẽ hơn cho việc dập tắt lửa và một sự đại tu phòng chữa cháy của thành phố.

“Thị trường đã không giải quyết vấn đề của các thành phố cháy”, Wysopal nói, tiên đoán rằng an toàn Internet có lẽ đòi hỏi một tai họa lịch sử để ép thay đổi. “Dường như đối với tôi thị trường thực sự sẽ không tự nó giải quyết vấn đề này”.

Nhưng đây là sự việc gây sợ hãi: Sự thúc đẩy tạo ra các tiêu chuẩn an toàn chống cháy mới ngặt nghèo đã không bắt đầu sau Vụ cháy Khổng lồ ở Chicago (Great Chicago Fire) vào năm 1871, vụ đã giết chết hàng trăm người và 100.000 người mất nhà cửa. Một vụ cháy thứ 2, gần 3

năm sau, vào năm 1874, đã buộc các quan chức ở Chicago cuối cùng phải tiến hành các thay đổi thực sự.

Câu chuyện của **Craig Timberg**

Video của **Jorge Ribas**

Các minh họa của **Harry Campbell**